

**PROGRAMA DE ESTUDIOS**



**INFORMÁTICA  
FORENSE**



# NUESTRO PROPÓSITO

## Transformar positivamente la vida de las personas

Queremos que seas protagonista en la transformación que estamos viviendo. Por eso, nos comprometemos a capacitarte para que estés al día con las necesidades digitales actuales.

Te invitamos a trabajar en conjunto para que descubras tu mejor versión y la potencies. Anímate, toma las riendas de tu futuro.





# Modalidad del Curso

## Duración

15 horas

## Frecuencia semanal

2 encuentros de 2 h

## Modalidad

Online en vivo

## Grupos reducidos

Promedio 15 personas

**NIVEL**

Avanzado

**REQUISITOS**

Es recomendable tener una base sobre:

- Introducción a la Ciberseguridad
- Criptografía y Blockchain





# CONTENIDO DEL CURSO

Domina las herramientas de trabajo de un Analista Forense Informático. Incorpora metodologías para poder formar parte de un equipo dentro de una Causa Judicial.

## Prácticas en clase

A lo largo del curso realizaremos distintas prácticas basadas en casos reales. Se llevarán a cabo ejercicios que permitan al asistente comprender la metodología que debe utilizar un Informático Forense al momento de realizar la labor. Poniendo en práctica diversas herramientas realizará la adquisición del disco rígido a peritar, recuperará archivos y particiones eliminadas, trazará una línea de tiempo a partir de los artefactos recolectados, investigará el historial de navegación, el caché y las descargas desde los diversos navegadores Web.

Del mismo modo que analizará los correos electrónicos involucrados, la memoria RAM del equipo en cuestión, junto con los archivos de paginación y de hibernación. Se establecerán los lineamientos para el armado del Informe final, ya sea para presentar internamente en la Organización como para ser presentada en una causa judicial.





# ¿QUÉ APRENDERÁS ?

- Fundamentos de la informática forense.
- Procesos involucrados en una causa judicial.
- Metodologías y herramientas de trabajo.
- Tipos de adquisición.
- Cadena de custodia.
- Análisis Forense.
- File Carving/Data Carving.
- Metadata de archivos.
- Trabajo con browsers y e-mails.
- Uso de Nirsoft y Sysinternals Tools.
- Técnicas de investigación con correos.
- Recuperación de archivos eliminados.





# PLAN DE ESTUDIOS

## 1 Introducción Informática

- Ciencias Forenses
- Informática Forense
- Metodología
- Marco legal
- Consultor Técnico, Perito de Oficio y Perito de Parte
- LiveCDs Forenses
- Artefactos
- Prueba Digital
- Evidencia Digital
- Criptografía aplicada a la Informática Forense
- Registro de Windows
- Buenas prácticas

## 2 Adquisición Forense

- Conceptos
- Adquisición física
- Adquisición lógica
- Adquisición directa
- Adquisición indirecta
- Adquisición por hardware
- Adquisición por Software



- dd como herramienta
- GUYSMAGER
- FTK Imager
- Preservación
- Cadena de Custodia

### **3 Análisis Forense**

- Conceptos
- Slack Space
- Recuperación de archivos borrados
- Recuperación de particiones eliminadas
- File Carving / Data Carving
- foremost
- photorec
- Línea de tiempo
- Autopsy
- Análisis de metadata de archivos

### **4 Browser y Correo electrónico**

- Conceptos
- Historial
- Cache
- Descargas
- Nirsoft
- Sysinternals Tools
- Distintos Browsers
- SQLite
- Cabeceras de correos



- Distintos clientes de correo electrónico
- Técnicas de investigación con correos

## **5 Análisis de Memoria e Informe Pericial**

- Conceptos
- Memoria RAM
- Archivo de Paginación
- Archivo de Hibernación
- Dump de memoria
- FTK Imager
- DumpIt
- Análisis de RAM
- Volatility
- Informe final







# ¿Por qué en **CEGOS?**



## **Garantía de Aprendizaje**

Puedes recurrir sin cargo adicional si necesitas reforzar conceptos, recuperar clases o no estás satisfecho, puede ser de forma total o parcial.



## **Profesores Expertos**

Profesionales certificados internacionalmente que trabajan con la tecnología y son referentes en su sector.



## **Plataforma Alumni**

Espacio virtual donde encontrarás todo el material educativo, recursos, videos de clases grabadas, evaluaciones y más.



## **Orientación Profesional**

Ingresa al mundo laboral, crea un CV que impacte, comparte tu portfolio en LinkedIn y realiza simulacros de entrevistas.



## **Bolsa de Trabajo**

Postula a empresas líderes en su rubro que buscan talento en Latinoamérica y el mundo.



# MODALIDAD ONLINE EN VIVO

El aprendizaje a distancia en CEGOS está basado en la enseñanza presencial, un instructor dicta las clases utilizando un aula virtual en un horario establecido, las clases duran entre 2 a 3 horas de Lunes a Viernes y Sábados de 3 a 4 horas, las mismas se desarrollan en tiempo real donde podrás interactuar con el instructor y tus compañeros, se maneja cupos reducidos para que puedas tener un seguimiento más personalizado durante tu aprendizaje.

## BENEFICIOS

- Material digital en plataforma Alumni.
- Acceso ilimitado a plataforma educativa.
- Videoconferencia en tiempo real.
- Grabación de clases ejecutadas.
- Docente certificado internacionalmente.
- Certificado de aprobación emitido por CEGOS.
- Factura impuestos de ley.
- Garantía de aprendizaje.



## CERTIFICACIÓN

- Rúbrica de autoridades competentes
- Datos personales del alumno
- Carga horaria
- Plan de estudios
- Nota final

